

**Testimony of Chief Noel Cunningham, Principal of the MARSEC Group and the recently retired Director of Operations and Chief of Police of the Port of Los Angeles to the House Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity
March 16, 2006**

Mr. Chairman and Members of the Committee, thank you for inviting me to testify before you today. I will be discussing the proposed “Security and Accountability For Every Port Act” or “SAFE Port Act.” During this testimony I will address the act, and discuss other actions that I believe are critical in addressing vulnerabilities associated with maritime security. My assessment is based on my 40 years of experience as a law enforcement officer, Chief of the Port of Los Angeles Police, and Director of Operations at the largest port in the United States. My testimony is also being provided from my vantage point as a Principal of The Marsec Group – a small group that provides maritime and supply chain security consulting services to public and private sector clients.

I should also note that this testimony was prepared with the assistance of the two other principals from The MARSEC Group: Captain John Holmes, former Captain of the Port of Los Angeles – Long Beach and Dr. Charles Massey, who retired recently from Sandia National Laboratories as the program manager for the Department of Energy Second line of Defense Program. As you may be aware, Captain Holmes and Doctor Massey have significant experience in port and border security, and like myself were “in the field” during and after the tragic events of September 11th.

Having had the opportunity to review the SAFE Port Act, I would like to commend the committee for its efforts, and go on record as supporting the concepts embraced in the act. I wholeheartedly support the efforts outlined in the areas of strategic planning, information management and data integration. I am pleased to see that the bill addresses existing concerns regarding trade reconstitution. I am also very encouraged by the fact that the bill will better define the GreenLane process and that it embraces the use of a common metric in the Port Security Grant process.

My experience leads me to believe, however, that the act could be made significantly more effective if this committee expanded its scope to establish new priorities for existing programs that are critical to the security of our ports. These include port user identification, enhanced inspections in foreign ports, and security system integration at the port, regional and national level.

It is clear that the purpose of the “SAFE Port Act” is to improve maritime and cargo security, thereby protecting the safety and security of our citizens, our nation, and its economy. With over 80 percent of international trade volume carried by the maritime system, the likelihood that it will be targeted in the future by terrorists should be assumed. Although a great deal of discussion has taken place regarding whether maritime shipping is an appropriate means of transportation for a weapon of mass destruction, I firmly believe that this discussion misses the mark. If one is looking for a means of transport for a WMD there may be better vehicles. If one is looking for a means to cripple our economy, the transportation system is an exceptional target.

Past terrorist attacks against an oil tanker and a LNG carrier would seem to support that the marine transportation system is both the “target” and the “arrow”. To combat the terrorists and deploy systems to win the war on terror, the United States must aggressively support security programs already underway while implementing new ones to deal with the dynamic threat posed by modern day terrorists.

Although the “SAFE Port Act” proposes a set of initiatives to complement, and/or improve several existing maritime security programs, it is critical that an assessment of existing programs is conducted in order to identify and fill fundamental security gaps. The “SAFE Port Act” includes this crucial element and requires the development of a Strategic Plan to deal with the threat and ensure that security efforts are focused on the right issues. Equally important, given the likelihood of an attack on the maritime system, is an understanding of how the system will be restored after an attack. I am pleased to see that the Act addresses this important issue.

I am encouraged to see that the bill addresses the critical issue of research and development. It is my strong belief that our focus needs to transcend our current efforts at plugging the security gaps that we know, and embrace the identification and prevention of those that currently do not exist. If this is going to be done, intelligence gathering and research and development will be key elements in the success of these efforts. Although I am heartened by these areas of focus, I would like to see the Act expanded to specifically embrace all methods of cargo scanning including those that have proven to be most problematic up to this point, i.e. chemical and biological detection.

I also believe that the bill would be more comprehensive if the research and development section specifically addressed the issue of improving portable detection equipment. If we are truly going to embrace the concept of pushing back the borders and developing a multi-layered layered security system, it is critical that we not only conduct most of our inspections overseas (as is currently the focus of the Container Security and Megaports initiatives), but that we also provide our seagoing inspection teams the equipment that is needed to prevent illicit materials from being transported into and through U. S. waters. Seagoing examinations are hazardous undertakings. It is critical therefore that we develop equipment that is specifically made for the maritime environment.

Although I recognize that this issue is generally addressed in some of the existing regulations, I would also like to support the idea of outlining requirements for training and exercises in the bill. As a career law-enforcement officer I can not underscore enough the criticality of a solid training program. It is my belief that this bill should require ports and port personnel to take a leadership role in port security training. Requirements should be put in place requiring port and regional training exercises in such areas as response, personnel evacuation and reconstitution of operations.

It is my belief that when an assessment is conducted, key gaps will be identified. These include:

- Inability to clearly determine who is working in our ports: Unlike our airports, our ports have no credentialing system. One of the universal truths in law enforcement is that security starts with people. Officers and responsible citizens are oftentimes much more reliable and accurate in detecting and deterring criminal, or terrorist, activities than sophisticated technological systems. If bad people can not undertake their efforts

without being exposed, the system will be more secure. Identification of workers through efforts like the Transportation Worker Identification Card (TWIC) are on target and expansion of this type of information assessment and utilization to other members of the supply chain, including shippers, carriers, freight forwarders, and creditors, as mandated by this Act will improve security. However, issues associated with the privacy of the data will need to be addressed. Through a cooperative effort involving labor, the industry, and the government, I believe the important “information” component of the maritime system – a component that would include information about the cargo and the people involved in its purchase and movement - can be used to make the system more secure. Credentialing and access control are the foundation of any effective security system. This program needs to become the highest security priority.

- Inability to truly know what is in the containers arriving in the U.S: As my close friend and colleague, Dr. Stephen Flynn has stated, the question that must be asked is “what’s in the box?” Given the complexity of the supply chain and the number of individuals involved, the only means to truly ensure that the contents of the container do not pose a threat is to use technology to screen the contents. In order to truly embrace maritime security, this screening must be forced to occur prior to loading. At present the amount of foreign inspections is simply not significant enough to provide a deterrent effect. No Port Chief of Operations or Coast Guard Captain of the Port wants to be the individual who finds the dirty bomb after it is offloaded in his or her port.
- Lack of integration of current security systems on the port, regional and national level: In the post 9/11 climate ports and terminals have embraced the use of security systems that include, cameras, access control and intrusion detection systems. Unfortunately there are few cases where ports have taken the lead, and/or found the funding to integrate these systems. As a result, knowledge of security breaches or attempted breaches are not known outside the identifying system, nor are they examined systematically. What currently exists in most ports is a conglomeration of individual hardware, and not a port-wide security system.

The gaps identified represent fundamental security shortfalls that must be addressed. Access control and overseas screening are foundational to supply chain security, and they represent the most efficient means to push back the borders. Until shortfalls such as these are rectified, the security of the entire supply chain must be called into question.

While the use of information assessment tools and sophisticated detection systems by government agencies are two important legs of the three-legged security stool, system security will not be achieved unless the last leg of the stool is accounted for. This leg consists of the major players in the maritime transportation system – labor, terminal operators, shippers, carriers, and port authorities. Involvement of these stakeholders has been pursued through initiatives such as the Customs-Trade Partnership Against Terrorism (C-TPAT). I am pleased to see that the “SAFE Port Act” wisely endorses this effort.

I believe the shipping industry wants to do more in the area of security. Because they are in business, they must be able to justify some of the expense and I believe they are right to expect

something in return for their investment. For example, businesses that invest in the security measures required for participation in C-TPAT should be given priority in clearing their cargo through customs over business that do not. Designation of a GreenLane with achievable and definable requirements will do much to persuade businesses to invest in processes and technologies that can make us more secure.

The involvement of industry is also crucial from another aspect. No one knows better where the security vulnerabilities are in the maritime industry than the industry. Tapping into this knowledge base is crucial for success. Operation Safe Commerce, of which my partners and I were key participants, is an example of industry helping to determine where security efforts are best placed. The “SAFE Port Act” continues to support this crucial industry-led effort.

While container security is rightly the subject of much focus, cargo does not only move through the maritime system only in steel boxes. A Weapon of Mass Destruction (WMD) could also be transported to the United States on a bulk oil tanker, a Roll-on/Roll-off vessel, or a fishing trawler. Security of our nation depends on systems that will deal with all types of maritime threat delivery vehicles and targets. I am please to see that the focus of the bill goes beyond containerized cargo and that research, development and testing of processes and technologies that will address prioritized threats throughout the maritime system, are included in this Act.

I also believe that if one is going to address security needs, the issue of resources can not be ignored. A question that must be asked during the planning and analysis required in this bill must be: “Are the federal, state and local resources on hand sufficient to educate, deter, detect, respond, and recover in the manner expected?” I think that the unfortunate answer to this question will be “no”. I, more than most, realize that priorities must be established based on the principals of risk management. I have lived this reality for over 40 years.

Unfortunately, when organizations become driven more by funding parameters than risk management principals, adjustments need to be made. This is the situation we now find ourselves in. As such, I implore you to include, as part of the planning requirements in the bill, a match of the mission requirements and resources needed.

I would once again like to commend the Committee for your efforts. I can see that a great deal of work and thoughtful analysis has gone into this project. I am convinced that if additional security concerns are addressed in areas such as port user identification, overseas inspection, and security integration, the Act has the ability to significantly enhance port, maritime and supply chain security. I would like to offer the assistance of my colleagues and myself to support you in any way possible in moving this critical Act forward.

Thank you. I would be happy to answer any questions you may have.